



Secure Software Development

Agenda

- I. About NIC MX
- II. Introduction
- III. Securing Code/Data
- IV. Securing Passwords

I. About Us

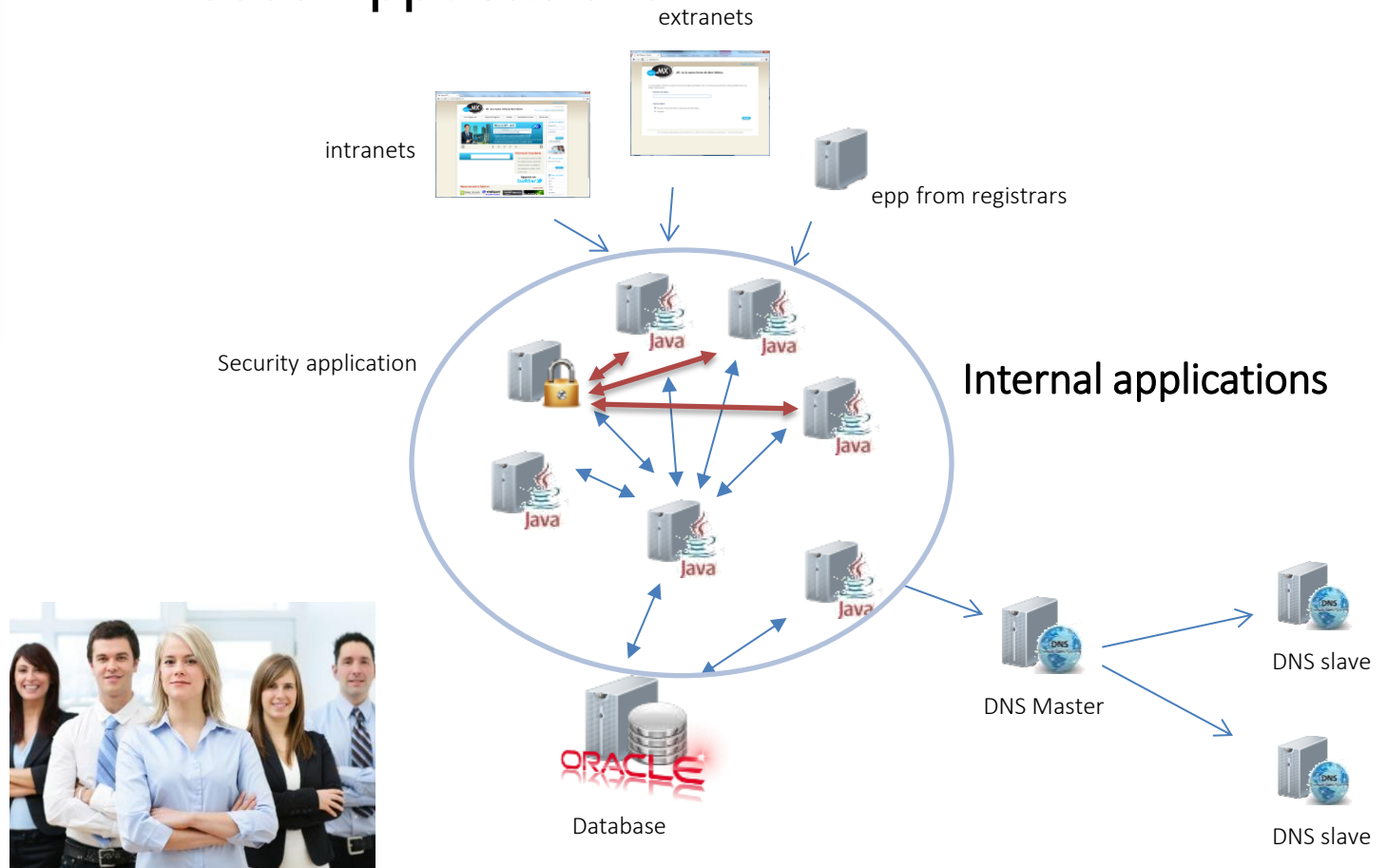
- ccTLD for Mexico, part of LACNIC
- More than 130 employees
- ~700,000 .MX domain names (2014)

Statistics	
.com.mx	442,228
.gob.mx	7,404
.net.mx	362
.edu.mx	9,724
.org.mx	19,130
.mx	227,708
TOTAL	706,556



II. Introduction

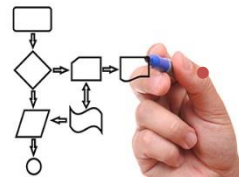
- In-house Applications



II. Introduction

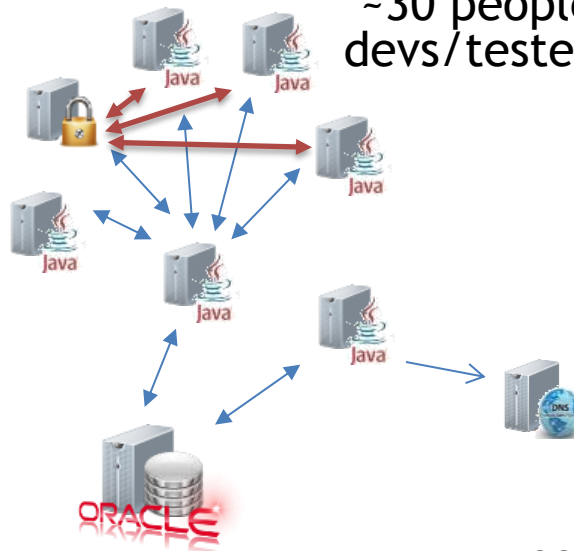
- Different environments with same configurations...

Development



~40 apps

~30 people
devs/testers

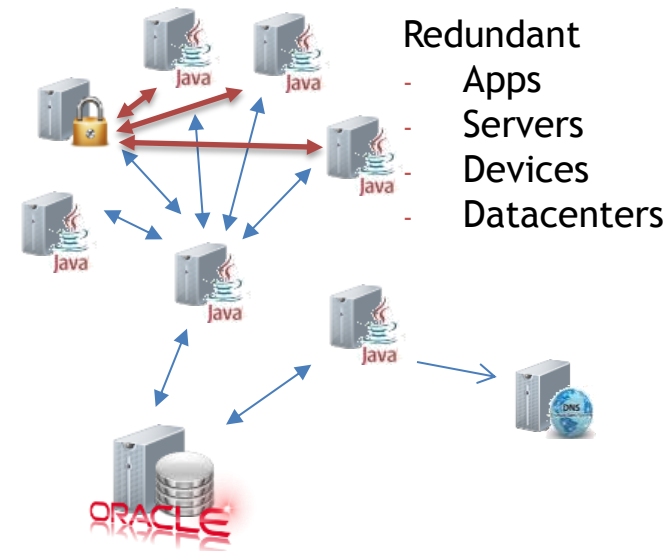


scalability

Production



~120 app
instances

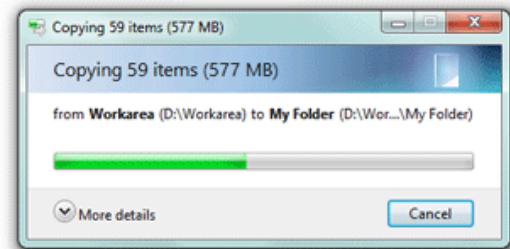


II. Introduction

Possible **Risks...**



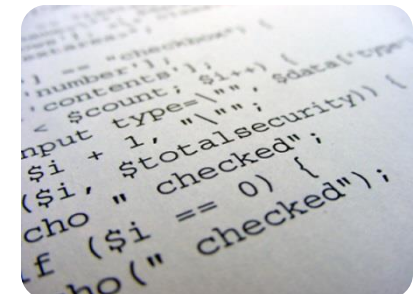
- **Code Leaks**
- **Unauthorized access to Sensitive Data from Development environment**
- **Compromised passwords**



II. Introduction

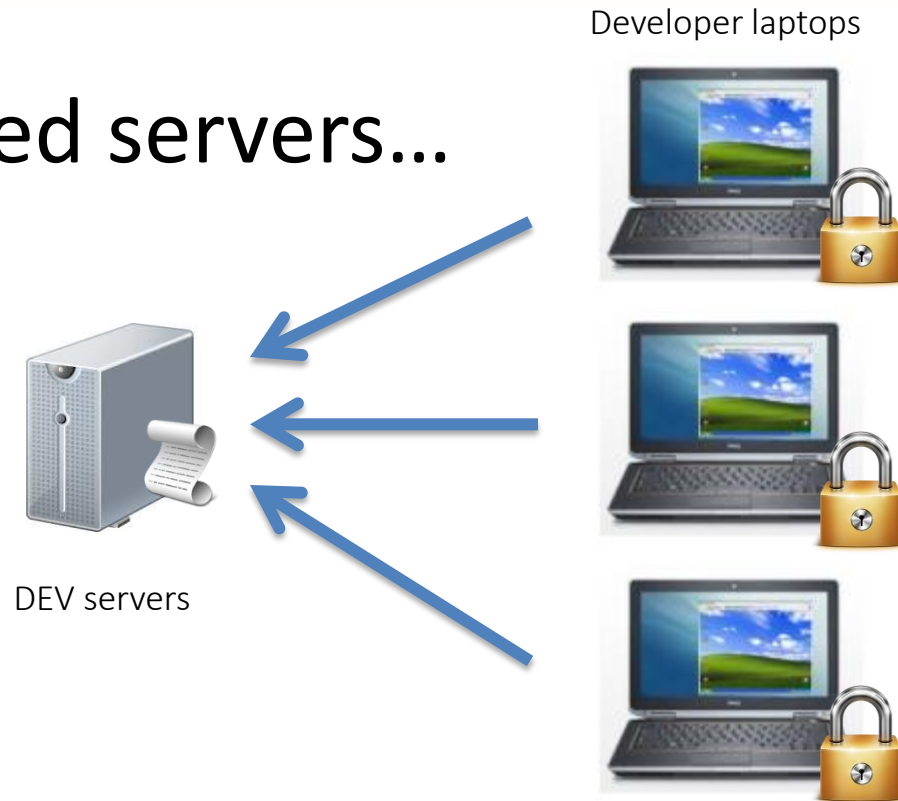
Measures to...

- Secure code
- Secure data
- Secure passwords



II. Securing Code/Data

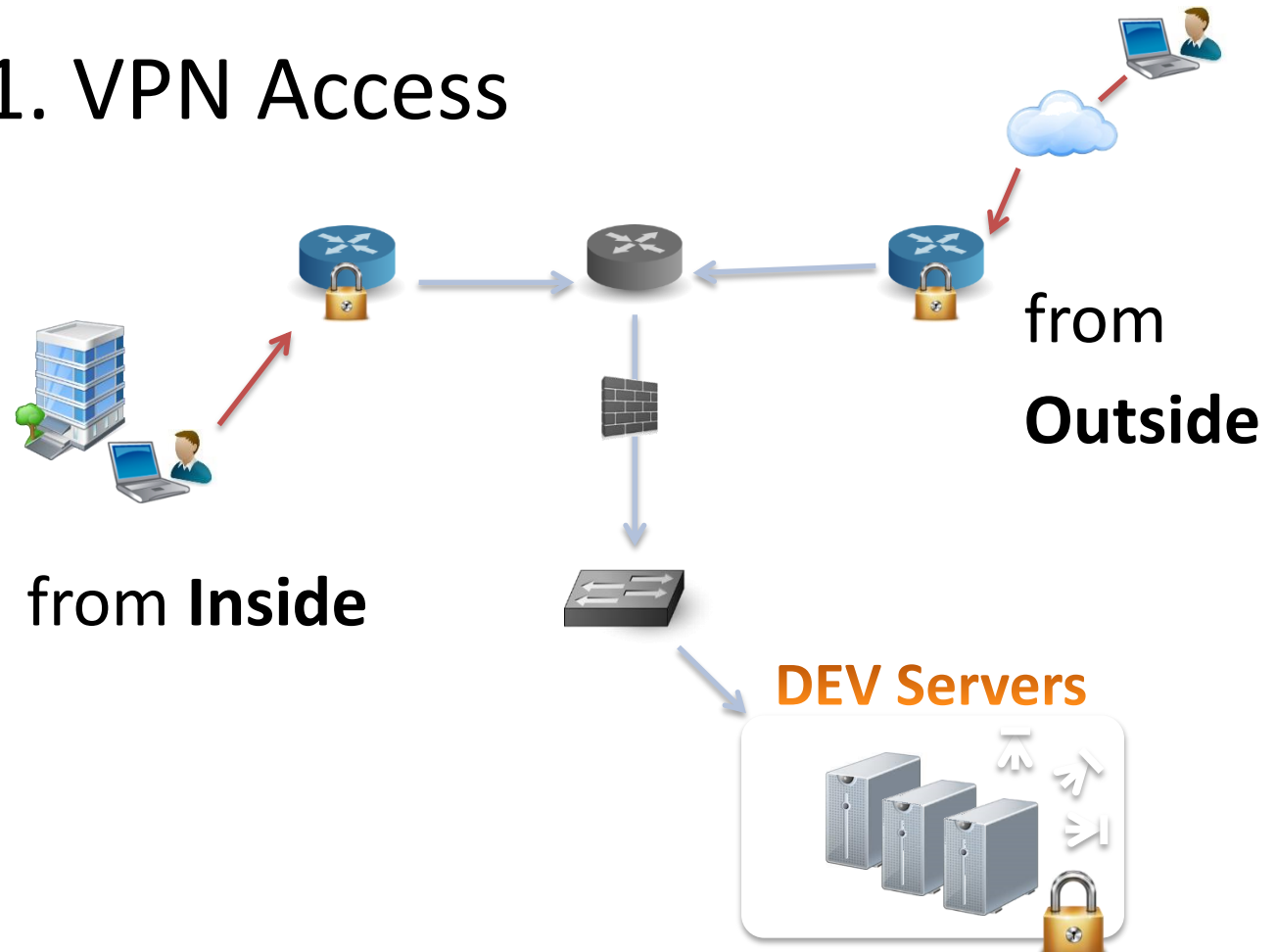
Isolated servers...



...with **copy restrictions**

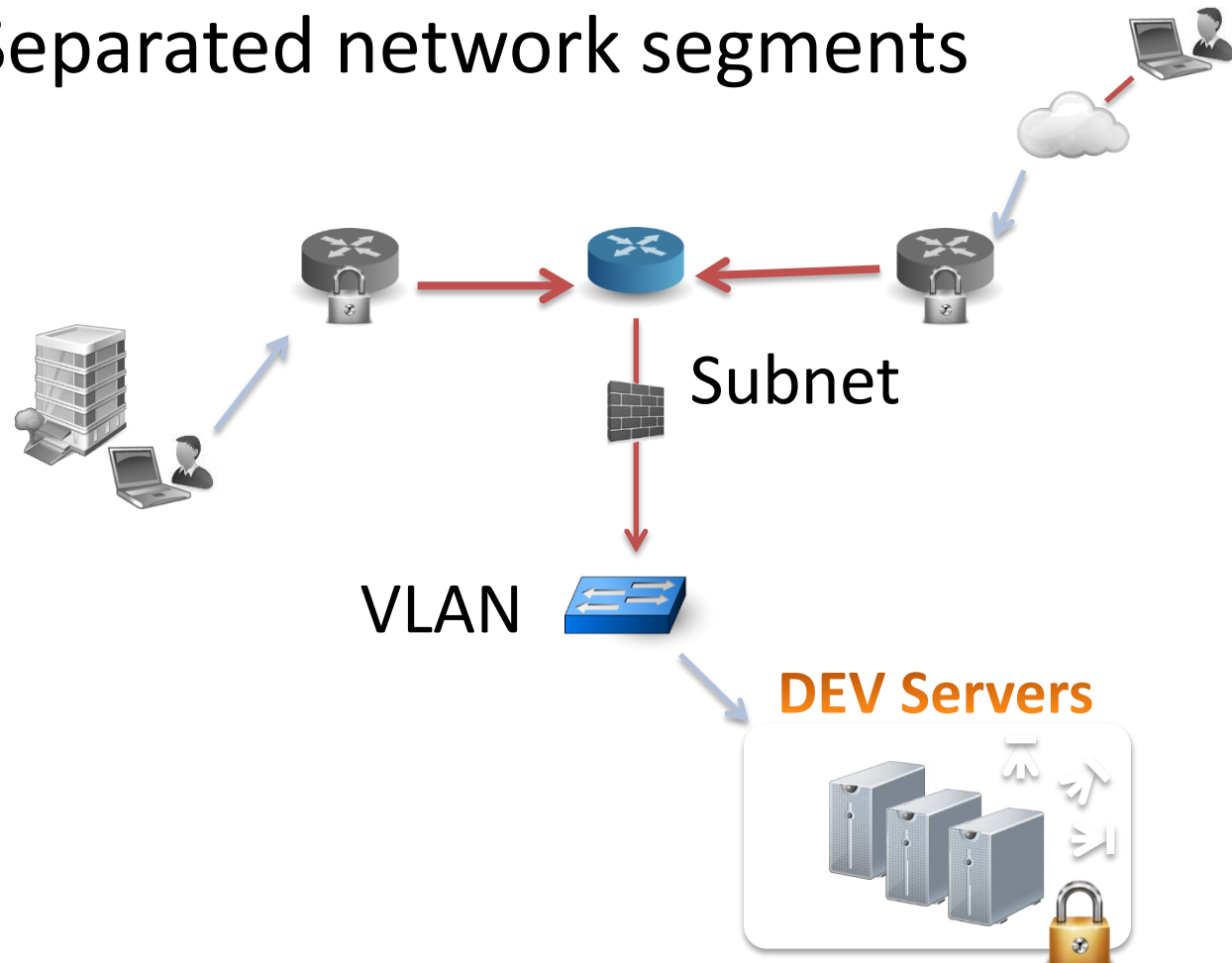
II. Securing Code/Data

1. VPN Access



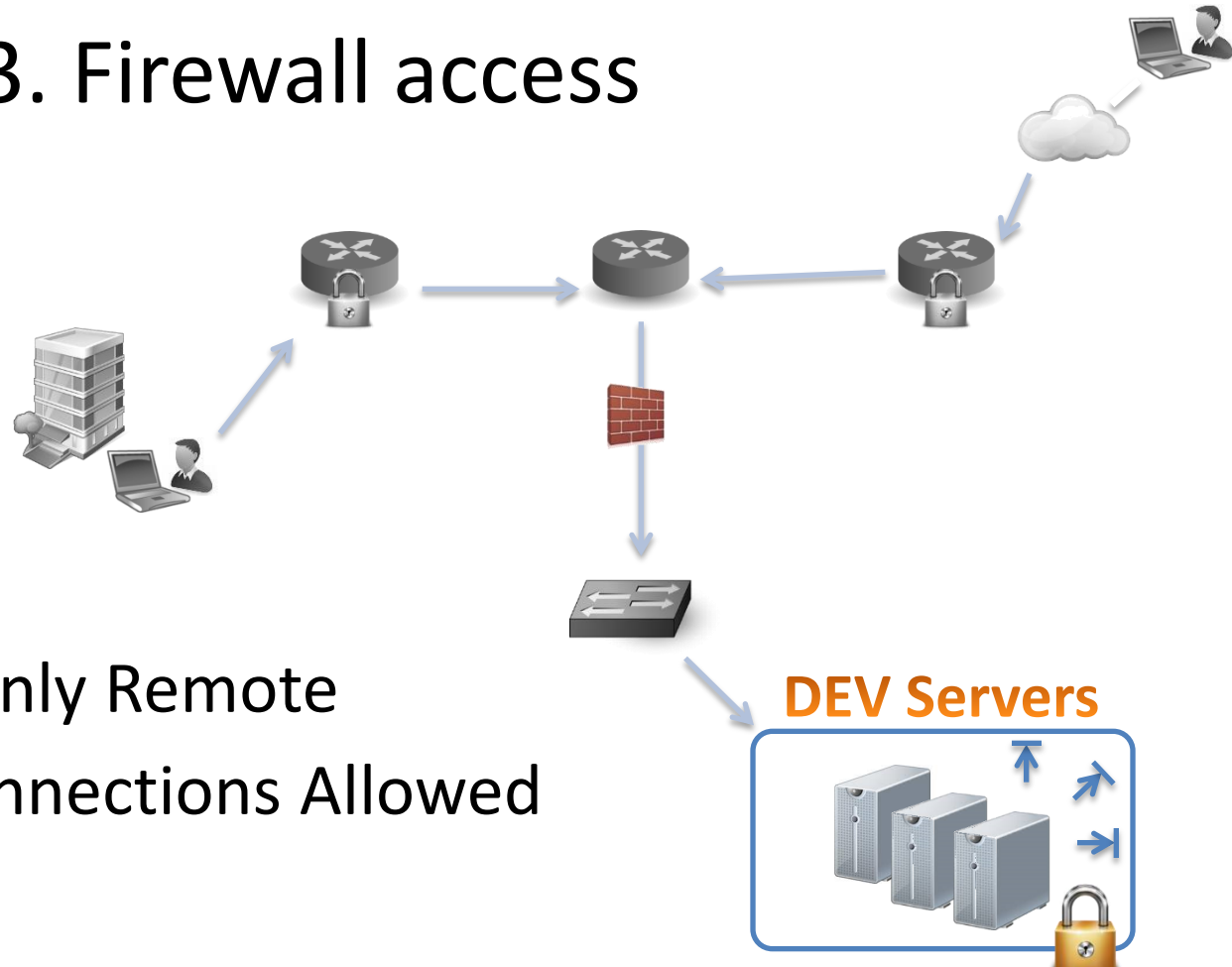
II. Securing Code/Data

2. Separated network segments



II. Securing Code/Data

3. Firewall access



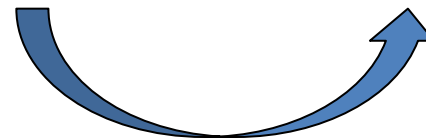
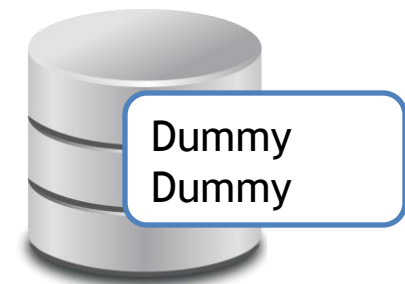
- Only Remote
Connections Allowed

II. Securing Code/Data

Dummy Data in...

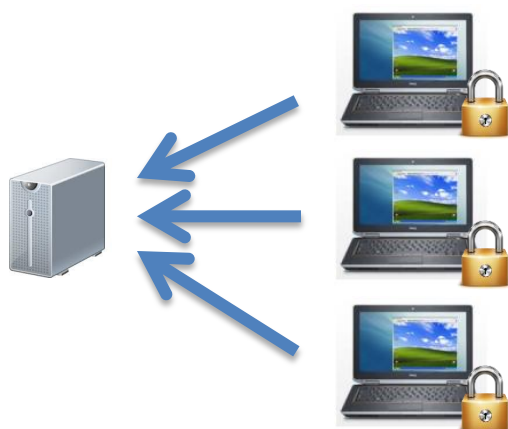
Production

Development



Periodic refresh of data

II. Securing Code/Data



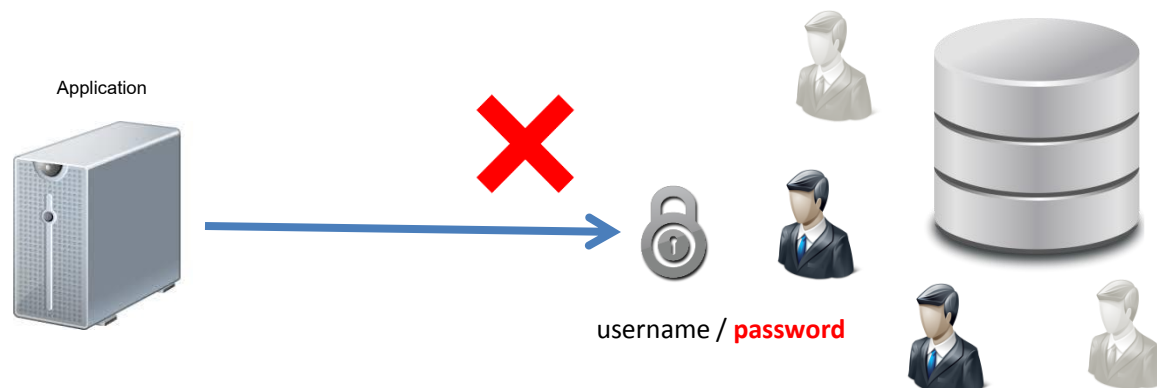
Advantages



- Code is safe from being copied.
- Data is protected.
- Access controlled to resources.

III. Securing passwords






When applications need
access to resources...



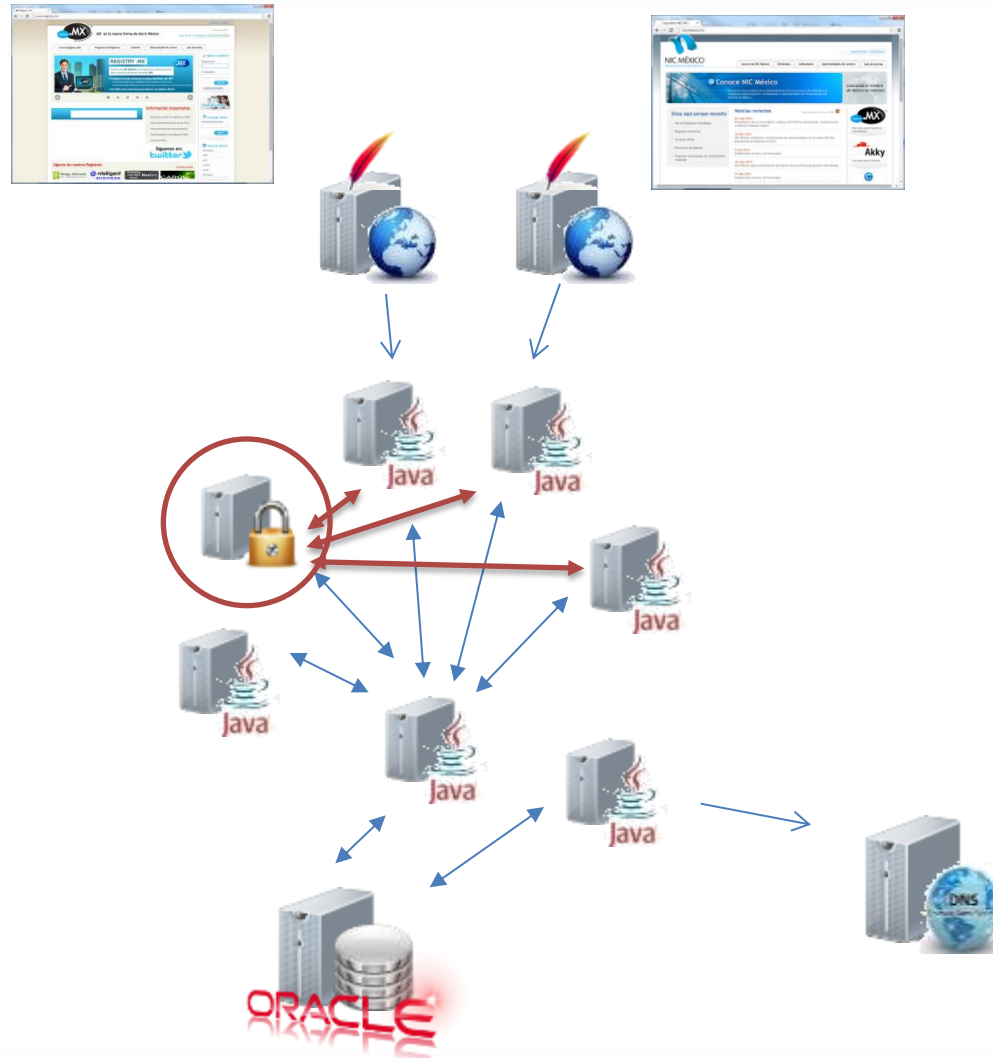
- Database Passwords
- Certificate phrases
- Password for provider's services
- etc

III. Securing passwords

How an application gets its credentials?

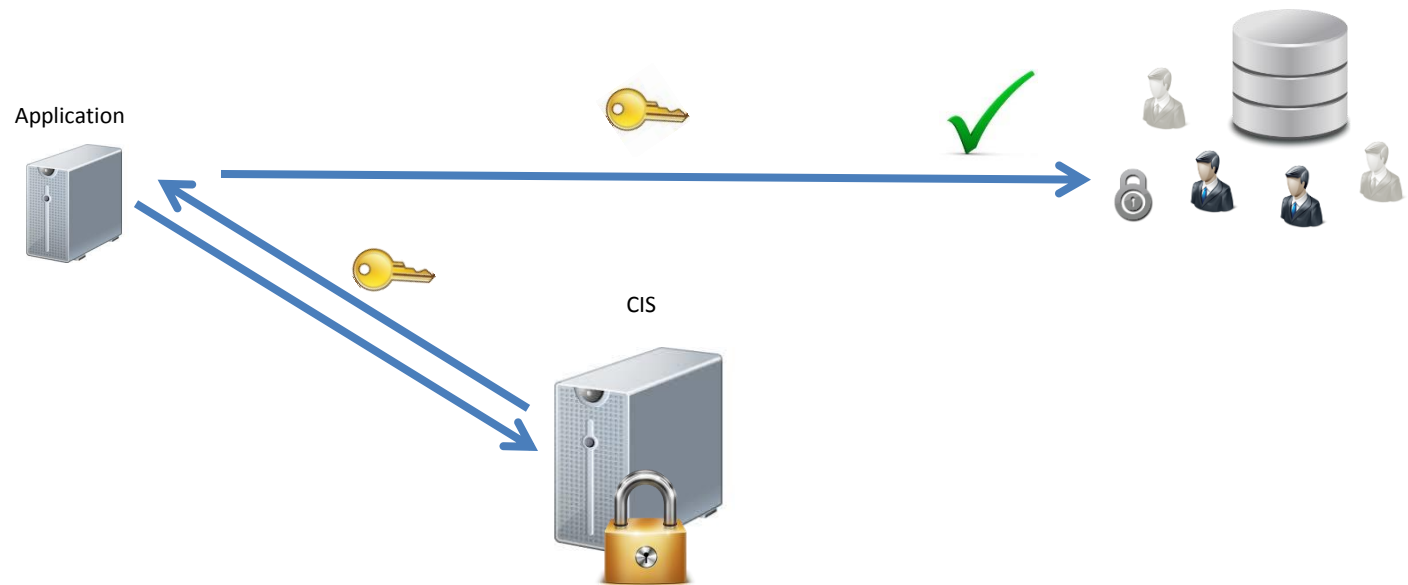
			
1°	 Config. File	Starts fast	Easy to steal
2°	 Encrypted & Ask for creds	Hard to steal	Hard to admin (many servers)
3°	 Centralized app	Hard to steal Easy to admin	One point of failure

III. Securing passwords



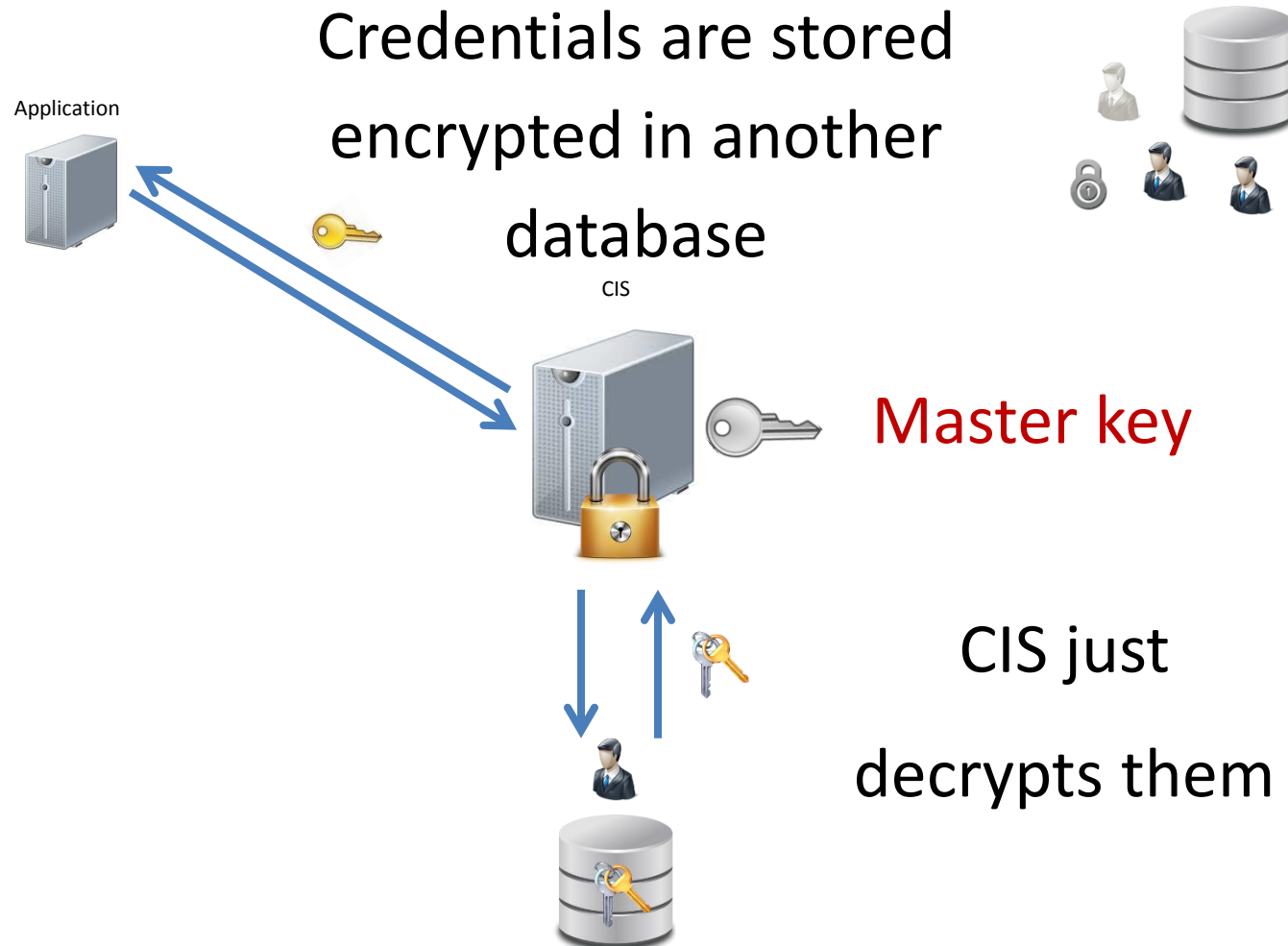
III. Securing passwords

CIS (Credential Information Service) provides credentials to applications



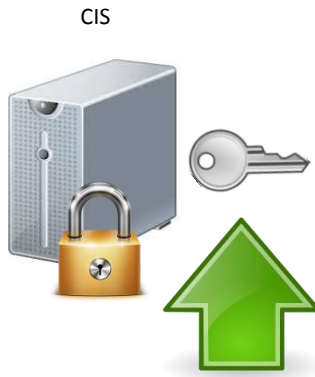
However, it doesn't store passwords

III. Securing passwords



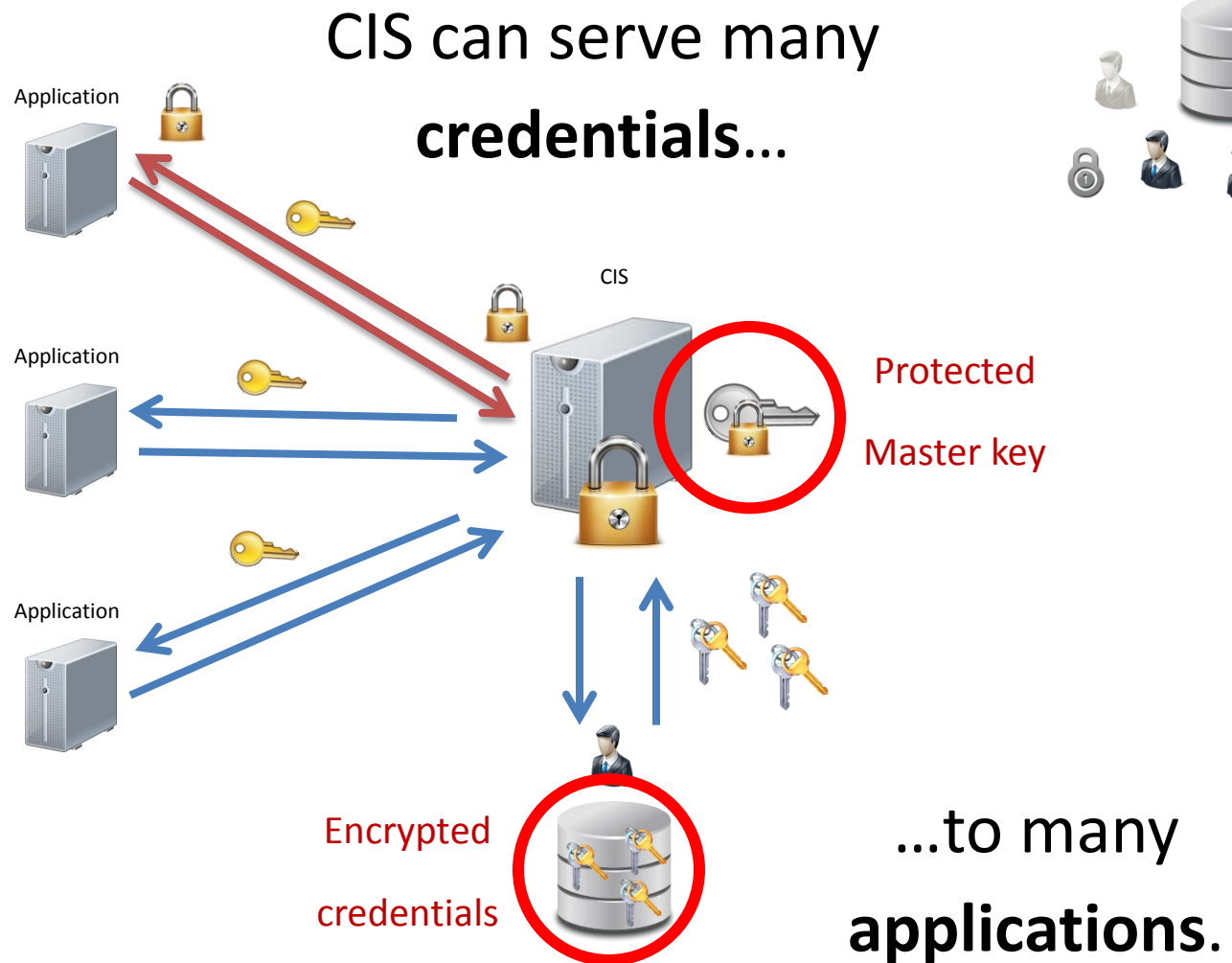
III. Securing passwords

A **Master Phrase** must
be typed **by an
Administrator** when CIS
starts



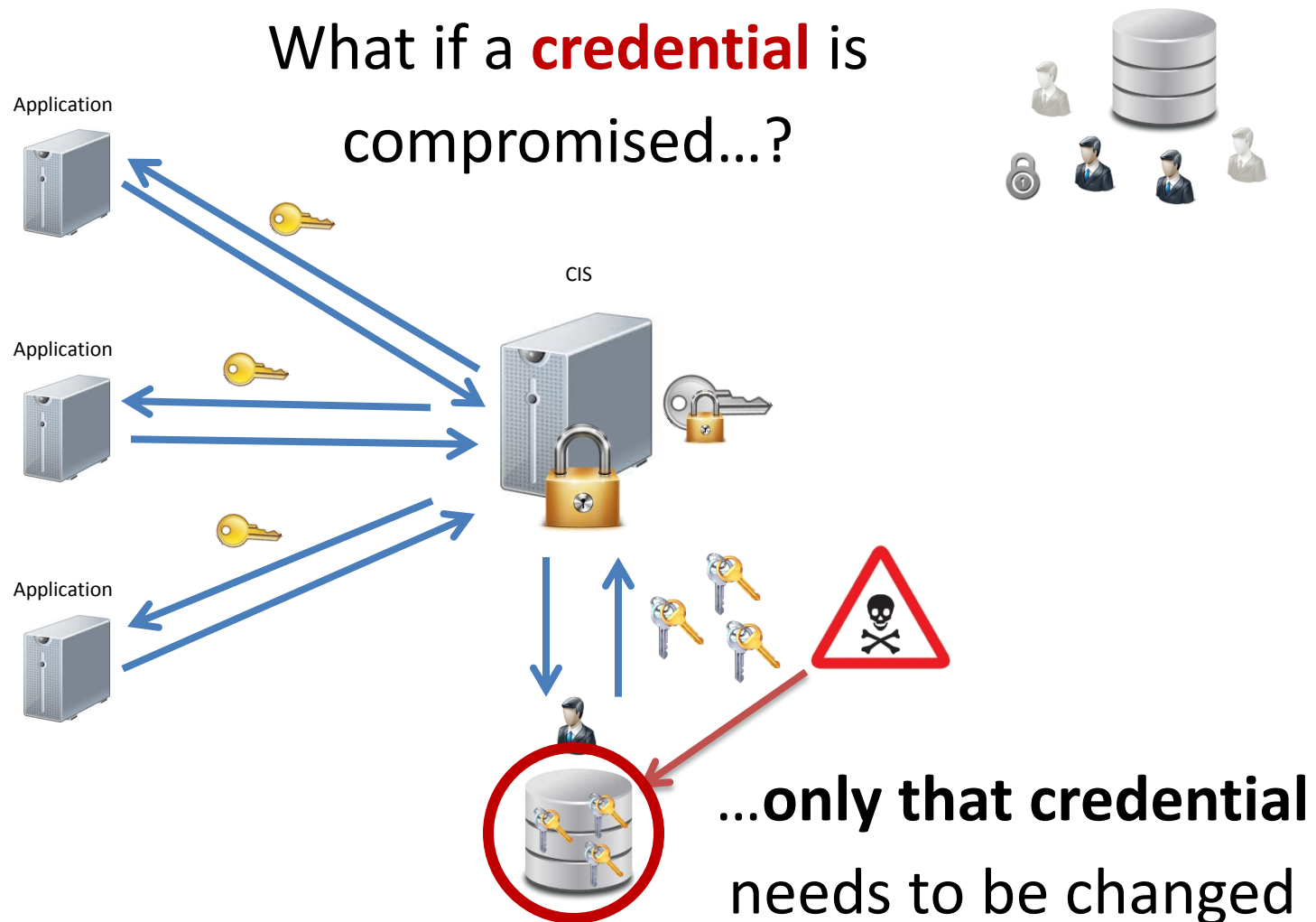
...and It remains loaded
in Memory

III. Securing passwords



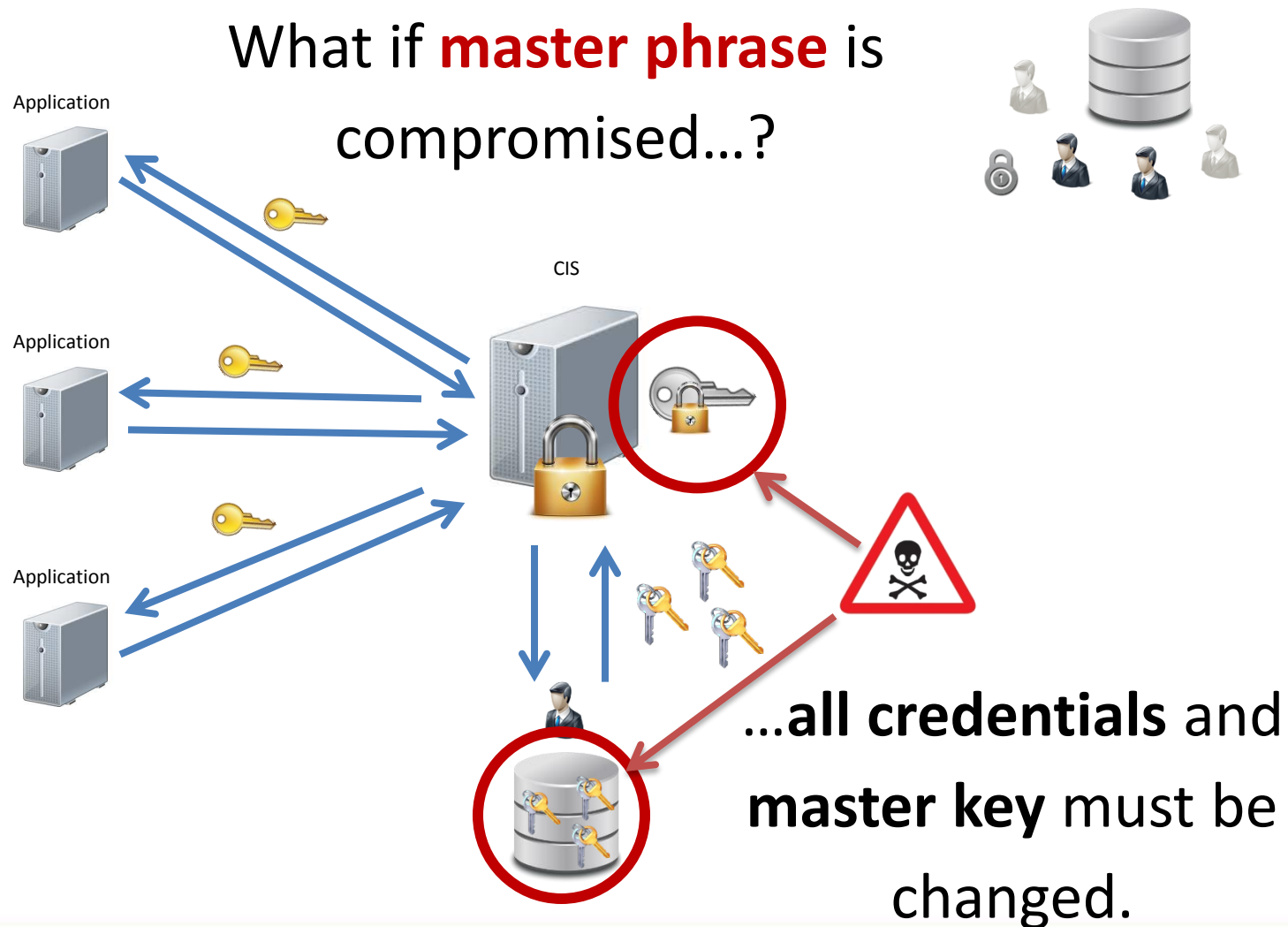
III. Securing passwords

What if a **credential** is compromised...?

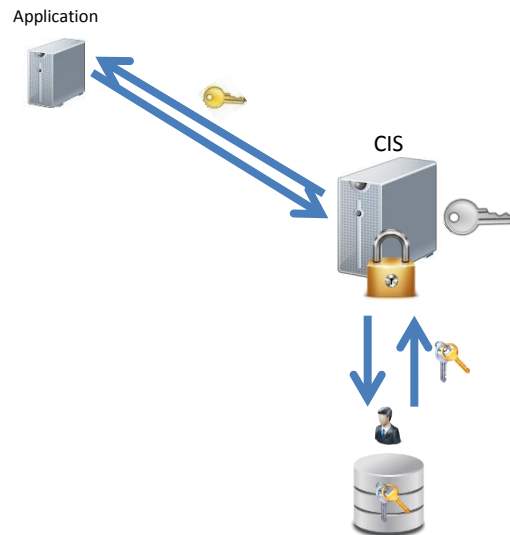


III. Securing passwords

What if **master phrase** is compromised...?



III. Securing passwords



Advantages



- Only one point of failure
- Nobody knows passwords
- Easy to change passwords if **someone leaves** or a **credential is compromised**

Questions?



Thank you!

Carlos Cardenas